UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,125	07/07/2003	Kyung-Hun Jang	249/387	7220

27849 7590 02/02/2010

LEE & MORSE, P.C.
3141 FAIRVIEW PARK DRIVE
SUITE 500
FALLS CHURCH, VA 22042

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2435	

MAIL DATE	DELIVERY MODE
02/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/613,125	JANG ET AL.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,7-13,15-18 and 20-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7-13,15-18 and 20-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/10/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 11/10/2009 has been entered.

2. Claims 1-2, 4-5, 7-13, 15-18 and 20-25 are pending. It is noted that applicant did not submit a complete listing of the pending claims. In the future, the examiner respectfully asks that a complete listing of the claims be submitted with any response to minimize the chances that the wrong claims are examined or published when the application is ready for allowance.

3. Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Information Disclosure Statement

4. The NPL document listed in the IDS submitted on 11/10/2009 was considered.

Examiner's Comment

5. Please note on page 14 of Applicant's remark on 01/03/07, the Applicant states that the claims are now limited to tangible computer media as the spec no longer includes carrier wave. The examiner takes this a disavowal of that nonstatutory embodiment.

However, the examiner suggests the Applicant adding the limitation "non-transitory" to the claims 9-11 in order to be in accordance with the Office's current guideline regarding subject matter eligibility of computer readable medium.

Claim Objections

6. Claim 10 is objected to because of the following informalities:

As per **claim 10**, it recites a tangible computer readable medium having embodied thereon a computer program to carrying out the method of a canceled claim 3. The examiner believes this is an unintentional error. Since claim 3 is canceled and claim 10 is assumed canceled.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 1-2, 4-5, 7-9, 11-13, 15-18 and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. ("Key agreement in ad hoc networks", Computer Communications, Volume 23, Number 17, 1 November 2000) in view of Kadansky et al. (U.S. Patent No. 6,295,361) and further in view of Wong et al. ("Secure Group Communications Using Key Graphs", IEEE/ACM Transactions on networking, Volume 8, Number 1, February 2000, which is provided by the Applicant).

11. As per **claims 1, 7, 12, 20-23 and 25,** Asokan et al. discloses (a) generating a first group key (choosing a fresh password/weak shared password and sharing it among those present in the room – e.g. page 3 and initial password – e.g. page 4 Please note fresh password/weak shared password/initial password corresponds to Applicant's first group key) in N wireless terminals (forming an ad-hoc group (an ad-hoc meeting –e.g. p1, "They would like to set up a wireless network session…for the during of the meeting"), where N is equal to or greater than two (P5,

"There are two parties A and B which share a weak secret P" and P6 "We can slightly modify this….to a contributory multi-party protocol") ;

(b) generating an initial second group key in a main wireless terminal (a leader – e.g. P6) to perform a key distribution center function among the N wireless terminals in response to a request from one of (N-1) sub wireless terminals ("The leader will broadcast the message in step 1…An additional round will be needed for the leader to pick a common session key and distribute it to the members of the group...he shares with them" – e.g. page 6. Please note on pages 5-6 of Asokan et al. reference, "In step 1 A sends Ea encrypted with the weak secret P...One obvious way to extend this protocol to the multi-party case is to elect a leader", which met the claimed limitation of a request from one of (N-1) sub wireless terminals) the request being communicated using the first group key, and transmitting the initial second group key to (N-1) sub wireless terminals (P6, "An additional round will…to pick a common session key and distribute it the members of the group….he shares with them". Asokan et al. also discloses on page 3, "1.3 Password-based Authenticated Key Exchange…by choosing a fresh password and sharing it among those present in the room…Therefore, we need a protocol to derive a strong shared session key from the weak shared password" – e.g. page 3. Please note a strong shared session key corresponds to Applicant's second group key. Asokan et al. further discloses on page 4, "The basic secrecy requirement is that only those players that know the initial password should learn the resulting session key, which met the claimed limitation of the request being communicated using the first group key. In other words, the requesting member must prove his/her membership in the request by using the initial password (i.e. first group key); and

(c) encoding data using the initial second group key, and transmitting the encoded data between the N wireless terminals (P4 "In a landmark paper [4], Bellovin and Merrit….encrypted key exchange (EKE) and P5 "But the basic form of the generic protocol remains the same." Inherently, Asokan et al. teaches after the protocol is complete, the multi parties must communicate using the session key (the second group key) to encoding data and transmitting the encoded data among the N wireless terminals since the protocol is using encrypted key exchange (EKE), a well known protocol invented by Bellovin and Merrit disclosed on the P4 of the Asokan et al. reference).

Asokan et al. does not explicitly disclose modifying old group key (i.e. the initial second group key) in the main terminal according to a modification time period, predetermined in the main terminal, and (e) transmitting the at least one new key (i.e. modified second group key) to the (N-1) sub terminals, wherein at least one new key (i.e. modified second group key) is transmitted and used to encode data between the N terminals during a session/predetermined time period (i.e. use of the first group key). However, Kadansky et al. met the claimed limitation by teaching Key manager node (a network entity in charge of key distribution and management) may change the group key at regular predetermined intervals (e.g. col. 7, lines 21-23). Key manager unicasts the new group key to the requesting group member via any appropriate key distribution mechanism and the key distribution mechanism can encrypt the group key when it is sent between the key manager and the group member (e.g. col. 7, lines 54-65). The group members may use the new group key and the old group key for a predetermined period of time (e.g. fig. 7 and col. 9, lines 51-53). The group key is a shared secret key, as is known to the persons of ordinary skill in the art using DES encryption method (e.g. col. 4, lines 60-65).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Kadansky et al.'s modifying old group key (i.e. the initial second group key) in the main terminal according to a modification time period, predetermined in the main terminal, and (e) transmitting the at least one new key (i.e. modified second group key) to the (N-1) sub terminals, wherein at least one new key (i.e. modified second group key) is transmitted and used to encode data between the N terminals during a session/predetermined time period (i.e. use of the first group key) into Asokan et al.'s in order to enhance group communication security by limiting the lifetime of a group key and to process out of order packets by using both the new and old key for some predetermined time.

Asokan et al. – Kadansky et al. does not explicitly disclose encodes the new group key (i.e. initial second group key, modified second group key) using an old group key (i.e. first group key, initial second group key) and transmits the encoded new group key (i.e. initial second group key, modified second group key) to the (N-1) terminals. However, Wong et al. met the claim limitation by disclosing server s generates a new group key, notify other users of the new group key, server s encrypts the new group key with the old group key and then multicasts the encrypted new group key to every user in the group (e.g. fig. 2 and page 13, right column, under section A Joining a Star Key Graph of Wong et al.).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Wong et al.'s encodes the new group key (i.e. initial second group key, modified second group key) using an old group key (i.e. first group key, initial second group key) and transmits the encoded new group key (i.e. initial second group key, modified second group key) to the (N-1) terminals into Asokan et al. – Kadansky et al. 's in order to securely

distributing new keys and protect new keys for confidentiality (e.g. page 13, right column, under section A Joining a Star Key Graph of Wong et al.).

As per **claims 2 and 13**, Asokan et al. – Kadansky et al. – Wong et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the first group key is generated using a group password of the ad-hoc group (P3, "choosing a fresh password and sharing it among those present in the room, P4 "In a landmark paper [4]….encrypted key exchange (EKE)…derive a strong and P5 "shared key starting from only a weak shared key")

As per **claims 4 and 15**, Asokan et al. – Kadansky et al. – Wong et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal is a creator of the ad-hoc group (P 18, "for example,…the leader Mn has a greater say in the final session key…before finding one that leads to a particular type of K" and "In some ad-hoc networks there may already be a natural leader or ordering").

As per **claims 5 and 16**, Asokan et al. – Kadansky et al. – Wong et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further inherently discloses wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal (P16, "Therefore, when there is no a.priori leader or ordering…The general approach…This computation can be car- and P17, "ried out…to their distance from the reference value" and P20,

"If groups are dynamic, the session key needs to updated when the composition of the group changes").

As per **claims 8, 17-18 and 24**, Asokan et al. further discloses:

if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal (Page 5, "B extracts Ea, generates R randomly, encrypts it with Ea, and returns it to A in step 2");

decoding the second group key request message, using the first group key, in the main wireless terminal (P5, "The goal of the protocol is for A and B to mutually authenticate each other based on P, and to agree on a strong session key K…each player will compute the session key as K=f(Sa, Sb)") ; and

creating a second group key according to the decoded second group key request message, in the main wireless terminal (P6, "an additional round…he shares with them").

As per **claim 9**, Asokan et al. – Kadansky et al. – Wong et al. discloses the claimed method of steps as applied above in claim 1. Therefore, Asokan et al. – Kadansky et al. – Wong et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 11**, Asokan et al. – Kadansky et al. – Wong et al. discloses the claimed method of steps as applied above in claim 8. Therefore, Asokan et al. – Kadansky et al. – Wong et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO -892).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435